

CLAIMS

1. A detector apparatus, comprising:

a fingerprint sensor having a receiving portion that is configured to accept an authentication article, the fingerprint sensor detecting one or more predetermined features of said authentication article and reading at least a portion of a fingerprint of a user.

2. The apparatus of claim 1, further comprising a feature detection sensor, in operative relation with the fingerprint sensor, that detects one or more of the predetermined features.

3. The apparatus of claim 1, wherein the fingerprint sensor is detachably coupled to a portable device comprising:

an interface for operably communicating with a computer system; and
a verification engine for operably communicating with the computer system for determining an identity of the user.

4. The apparatus of claim 2, further comprising an interface for operably communicating with a computer system.

5. The apparatus of claim 4, further comprising a verification engine in operative relation with the computer system, the fingerprint sensor, and the feature detection sensor for determining an identity of the user, wherein the fingerprint sensor provides:

a first signal to the verification engine, the first signal being derived from the portion of the fingerprint, and the feature detection sensor provides:

a second signal to the verification engine, the second signal being derived from at least one of the one or more predetermined features of the authentication article.

6. The apparatus of claim 5, wherein the verification engine comprises:

a database having a user storage, an authorization profile storage, and an audit log storage; and

a comparator engine for comparing:

the first signal indicative of the at least portion of the fingerprint with a first authentication signal corresponding to a stored copy of the fingerprint within the database, and

the second signal indicative of the at least one of the one or more predetermined features of the authentication article with a second authentication signal corresponding to a stored copy of the one or more predetermined features of the authentication article within the database to provide an authorization signal for a secured application which is communicatively coupled to the computer system.

7. The apparatus of claim 6, wherein the authorization signal selectively provides an access to the secured application to the user.

8. The apparatus of claim 3, wherein the verification engine comprises:
a database having a user storage, an authorization profile storage, and an audit log storage.

9. The apparatus of claim 3, wherein the portable device comprises a smart card.

10. The apparatus of claim 1, wherein the fingerprint sensor is removably attached to a computer mouse having an interface for operably communicating with a computer system.

11. The apparatus of claim 1, wherein the fingerprint sensor is removably attached to a trackball having an interface for operably communicating with a computer system.

12. The apparatus of claim 1, wherein the fingerprint sensor is detachably coupled to a camera.

5 13. The apparatus of claim 1, wherein the fingerprint sensor is detachably coupled to binoculars.

14. The apparatus of claim 1, wherein the fingerprint sensor is detachably coupled to a telephone.

10 15. The apparatus of claim 1, wherein the authentication article comprises a precious gem.

16. The apparatus of claim 15, wherein the precious gem comprises a diamond and the one or more predetermined features are selected from a group consisting of:

- a weight of said diamond;
- a size of said diamond; and
- an exterior surface profile of said diamond.

17. The apparatus of claim 16, wherein the fingerprint sensor is coupled to a smart card having an interface for operably communicating with a computer system.

20 18. The apparatus of claim 17, wherein the fingerprint sensor is coupled to a verification engine for operably communicating with the computer system for determining an identity of the user bearing said smart card.

25 19. The apparatus of claim 18, wherein the verification engine comprises:
a database having a user storage, an authorization profile storage, and an audit log storage.

20. A pointing device, comprising:

an interface for operably communicating with a computer system;

a base;

a trackball mounted upon the base;

5 an upper section, said upper section including at least one button formed substantially on a top surface of the upper section; and

10 a fingerprint sensor having a receiving portion that is configured to accept an authentication article, wherein the fingerprint sensor is mounted within the upper section for detecting one or more predetermined features of said authentication article and for reading at least a portion of a fingerprint of a user's finger in response to the finger positioned adjacent to said fingerprint sensor and the authentication article disposed in proximity to the receiving portion and readable by said fingerprint sensor.

21. The apparatus of claim 20, further comprising a feature detection sensor in operative relation with the fingerprint sensor, wherein the feature detection sensor detects the one or more predetermined features, or any combination thereof of the authentication article.

22. The apparatus of claim 21, further comprising a verification engine in operative relation with the computer system, the fingerprint sensor, and the feature detection sensor for determining an identity of the user, wherein the fingerprint sensor provides:

20 a first signal to the verification engine, the first signal being derived from the portion of the fingerprint, and the feature detection sensor provides:

a second signal to the verification engine, the second signal being derived from at least one of the one or more predetermined features of the authentication article.

25 23. The apparatus of claim 22, wherein the verification engine comprises:

a database having a user storage, an authorization profile storage, and an audit log storage; and

a comparator engine for comparing:

the first signal indicative of the at least portion of the fingerprint with a first authentication signal corresponding to a stored copy of the fingerprint within the database, and

the second signal indicative of the at least one of the one or more predetermined features of the authentication article with a second authentication signal corresponding to a stored copy of the one or more predetermined features of the authentication article within the database to provide an authorization signal for a secured application which is communicatively coupled to the computer system.

24. The apparatus of claim 23, wherein the authorization signal selectively provides an access to the secured application to the user.

25. A pointing device as recited in claim 20, wherein the fingerprint sensor is located beneath a particular one of the button positions.

26. A pointing device as recited in claim 25, wherein the fingerprint sensor includes a capacitive imaging array located at the particular button position contactable by the user's finger so that the user's fingerprint may be imaged by the capacitive imaging array.

27. A pointing device as recited in claim 26, wherein the fingerprint sensor is incorporated into an operable button located at the particular button position.

28. A pointing device as recited in claim 25, wherein:
the fingerprint sensor includes an optical imaging array; and

the particular button position includes a transparent material through which the user's fingerprint may be imaged by the imaging array.

29. The pointing device of claim 20, further comprising one or more additional biometric
5 sensors in operative relation with the fingerprint sensor.

30. A pointing device, comprising:

an interface for operably communicating with a computer system;

a base;

a trackball mounted upon the base;

an upper section, said upper section including at least one button formed substantially on
a top surface of the upper section; and

a fingerprint sensor having a receiving portion that is configured to accept an
authentication article, wherein the fingerprint sensor is mounted within the upper section for
detecting one or more predetermined features of said authentication article and for reading at
least a portion of a fingerprint of a user's finger in response to the finger positioned adjacent to
said fingerprint sensor and the authentication article disposed in proximity to the receiving
portion and readable by said fingerprint sensor; and

a verification engine for operably communicating with the computer system for
20 determining an identity of the user.

31. The pointing device of claim 30, further comprising a feature detection sensor in
operative relation with the fingerprint sensor, wherein the feature detection sensor detects the one
or more predetermined features, or any combination thereof of the authentication article.

32. The apparatus of claim 31, wherein the fingerprint sensor provides:

a first signal to the verification engine, the first signal being derived from the portion of the fingerprint, and the feature detection sensor provides:

a second signal to the verification engine, the second signal being derived from at least one of the one or more predetermined features of the authentication article.

5

33. The apparatus of claim 32, wherein the verification engine comprises:

a database having a user storage, an authorization profile storage, and an audit log storage; and

a comparator engine for comparing:

the first signal indicative of the at least portion of the fingerprint with a first authentication signal corresponding to a stored copy of the fingerprint within the database, and

the second signal indicative of the at least one of the one or more predetermined features of the authentication article with a second authentication signal corresponding to a stored copy of the one or more predetermined features of the authentication article within the database to provide an authorization signal for a secured application which is communicatively coupled to the computer system.

34. The apparatus of claim 33, wherein the authorization signal selectively provides an access to the secured application to the user.

20

35. A detector apparatus, comprising:

a fingerprint sensor disposed at a location such that when operating said apparatus in a normal manner, a user's finger of a user's hand rests in proximity to and readable by said fingerprint sensor for reading a user's fingerprint; and

25 a feature detection sensor in operative relation with the fingerprint sensor and having a housing that is configured to receive an authentication article, the feature detection sensor being configured to detect one or more predetermined features of said authentication article,

wherein the detector apparatus identifies the user according to the fingerprint and at least one of the one or more predetermined features from the authentication article.

36. A method for providing user access to a secured application, comprising:

5 reading the fingerprint of a user with a fingerprint sensor;
detecting one or more features of an authentication article with the fingerprint sensor;
analyzing at least a portion of the fingerprint to derive a first indication for verifying an identity of the user;

analyzing at least one of the one or more features of the authentication article to derive a second indication for authenticating the fingerprint; and

combining the first and second indications for selectively providing access to the secured application to the user.

37. A method, comprising:

reading a fingerprint of a user;
detecting one or more features of a precious gem;
analyzing the fingerprint to derive a first indication;
analyzing the one or more features of the precious gem to derive a second indication; and
combining the first and second indications for verifying an identity of a user.

38. The method of claim 37, wherein the reading the fingerprint includes:

plugging in a fingerprint sensor having a first surface into a smart card; and
positioning a finger proximal to the first surface of said fingerprint sensor.

39. The method of claim 38, wherein the detecting one or more features includes:

positioning the precious gem into a slot located proximal to the first surface of the fingerprint sensor; and

reading a featureprint of the precious gem to derive the one or more features of the precious gem.